IKEv2 es un protocolo moderno desarrollado por Microsoft y Cisco el cual ha sido elegido como el servidor VPN por defecto desde Windows 7 y desde El Capitan. Cuenta con una encriptación bastante fuerte, con una muy buena implementation de auto re-conexión ante un cambio de red y es muy fácil de configurar porque los clientes no requieren de software de terceros para conectarse; simplemente se rellena el usuario, la contraseña y la dirección del servidor y ya está.

Desde el punto de vista de la encriptación y con el objetivo de evitar ataques man-in-the-middle, IKEv2 se autentifica mediante un certificado X.509 usando firmas RSA o ECDSA muy fuertes. Después de que el canal de comunicación ha sido establecido los clientes deben autentificarse en el servidor con el correspondiente nombre y contraseña usando normalmente el protocolo EAP-MSCHAPv2. Esto significa que el cliente necesita verificar la autenticidad del certificado X.509 usando Autoridades de Certificación. Al igual que ocurre en las conexiones HTTPS de los navegadores, el certificado del servidor debe ser válido para que el cliente se autentifique correctamente.

Hay dos formas de obtener certificados:

1. Usar un certificado proporcionado por una autoridad reconocida por la mayoría de los sistemas operativos.
2. Crear un certificado auto-firmado y distribuir una autoridad de certificación propia a cada cliente que quiera conectarse al servidor.

Lo mejor es hacer lo del punto **1**, porque hace que las conexiones sean mucho más fáciles para los clientes al no requerir la importación de certificados en el sistema. El punto 2 es más complicado y no lo vamos a seguir en este hack. Vamos allá: